eCH-0219 Glossaire IAM

Nom	Glossaire IAM
eCH-nombre	eCH-0219
Catégorie	Norme
Stade	Définie
Version	1.0
Statut	Approuvé
Date de décision	2018-11-28
Date de publication	2019-02-06
Remplace version	-
Condition préalable	-
Annexes	eCH-0219-IAM-Glossaire_Document_auxiliaire.xlsx
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé IAM Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Thomas Kessler, Temet, thomas.kessler@temet.ch Adrian Müller, ID Cyber-Identity Ltd, adrian.mueller@cyber-identity.com
Éditeur / Distribution	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

La présente norme définit les termes les plus importants pour les solutions IAM dans la cyberadministration fédérale suisse. L'ensemble des normes eCH relatives aux domaines IAM s'appuient sur cette norme.

Les termes intégrés incluent les Stakeholders, les processus, les services jusqu'aux détails d'implémentation dans les solutions IAM fédérées et non fédérées. Les termes tirés de normes internationales actuelles sont mis en relation avec la terminologie définie dans un souci d'intelligibilité.

Table des matières

Remarque

En vue d'une meilleure lisibilité et compréhension, seul le genre masculin est utilisé pour la désignation des personnes dans le présent document. Cette formulation s'applique également aux femmes dans leurs fonctions respectives.

1 Introduction

Les processus administratifs en ligne présupposent des sujets dignes de confiance et donc une entente avec les partenaires administratifs. Le service de gestion de l'identité et de l'accès (Identity and Access Management, IAM) interne à l'organisation a jusqu'à présent garanti des services administratifs adaptés. Ils doivent être pris en compte lors de l'élaboration de solutions dans la cyberadministration suisse afin de permettre que les applications et services locaux puissent être utilisés par les organisations en interne comme entre elles. Cette norme définit les termes et notions fondamentales dans le domaine de l'IAM, servant ainsi de base à tous ceux qui élaborent des solutions dans le domaine de la cyberadministration.

1.1 Statut

Approuvé: Le document a été approuvé par le comité d'experts. Il a pouvoir normatif pour le domaine d'utilisation défini dans le domaine de validité donné.

1.2 Champ d'application

Les concepts et termes définis dans la présente norme offrent une synthèse terminologique des normes eCH existantes dans le domaine de l'IAM, qu'ils viennent consolider. Les termes intégrés incluent les Stakeholders, les processus, les services jusqu'aux détails d'implémentation dans les solutions IAM fédérées et non fédérées. Les termes tirés de normes internationales actuelles sont mis en relation avec la terminologie définie dans un souci d'intelligibilité.

1.3 Avantages

L'élaboration d'un glossaire, remis à jour à chaque nouvelle norme ou actualisation de norme, dans le domaine de l'IAM, permet d'améliorer grandement la qualité et la cohérence de toutes les normes dans ce domaine.

1.4 Priorité

Le chapitre 2 décrit les principaux concepts et termes dans le domaine de l'IAM limité à la cyberadministration et la E-Health.

1.5 Caractère normatif des chapitres

Les chapitres de la présente norme sont de nature soit normative, soit descriptive. Le tableau suivant illustre ce classement:

Chapitre	Description
1 Fehler! Verweisquelle konnte nicht gefunden werden.	**Descriptif**
2 Terminologie	**Normatif**

L'annexe A et l'annexe C sont également de nature normative. Toutes les autres annexes de

cette norme sont descriptives.

2 Terminologie

2.1 Fournisseur de Services de certification

Selon la SCSE [2]: il s'agit d'*«un organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des certificats numériques.»*

Synonyme: Certification Service Provider, prestataire de services de certification, organisme de certification pour les certificats numériques,

Termes génériques: Trust Service Provider (TSP), fournisseur de services de confiance (VDA)

2.2 Artefact

Les artefacts sont de petits objets de données structurés, qui sont délivrés par un prestataire de services IAM (Service Provider, IdP) et couplés à une authentification du sujet.

Exemples:

- Artefacts SAML [1]
- Signature électronique d'un document (dans le cas d'un Remote Signing Service)

2.3 Attribut / Attribute

Représentation sémantique d'une propriété prêtée à un sujet, qui décrit le sujet plus en détail. L'identificateur est également un attribut d'utilisation spéciale.

Un attribut se compose de méta-attributs; nom de l'attribut («pointure» par exemple), type d'attribut («nombre entier» par exemple) et valeur d'attribut («39» par exemple).

Dans le cas d'une représentation, l'E-Identity du représentant possède, pour une certaine période, une quantité d'attributs de l'E-Identity du sujet représenté.

Attributs personnels: attributs appartenant à une personne physique. Elle seule est habilitée à statuer sur la transmission de ses attributs.

Enterprise Attribute: attributs appartenant à une organisation. Cette dernière décide, dans le cadre des lois et contrats en vigueur, de la transmission de ces attributs. L'utilisateur en soi au sein de l'organisation est confiné à un rôle secondaire dans le cadre de cette décision. D'ordinaire, le sujet consent de façon implicite à la validation de ces attributs (signature contrat de travail par exemple), faute de quoi il ne pourrait d'office remplir sa fonction.

2.4 Attribute Aggregation

Dans «Attribute Aggregation and Federated Identity» [3], N. Klingenstein décrit plus précisément le terme d'Attribut Aggregation. Il entend par là le processus consistant à demander les attributs relatifs à une identité numérique connue auprès de différentes sources et à les compiler.

2.5 Attribute Authority (AA)

Dans l'environnement SAML, le terme Attribut Authority est utilisé avant tout comme synonyme d'Attribute Provider (AP) (voir 2.9).

Fournisseur d'informations qui met à disposition des attributs pour la STIAM Community par le biais de l'interface définie (STIAM Sender).

Synonyme: Attribute Authority (engl.), Attribute Provider (AP)

2.6 Demande d'attribut

Une demande d'attribut permet de demander des attributs pour un sujet. Le résultat d'une demande d'attribut est une confirmation d'attribut (voir **Fehler! Verweisquelle konnte nicht gefunden werden.**).

La demande d'attribut peut être combinée à une demande d'authentification (voir **Fehler! Verweisquelle konnte nicht gefunden werden.**).

2.7 Confirmation d'attribut

Confirmation de la valeur d'un attribut par une Attribut Authority.

Exemples:

SAML 2.0 Attribute Assertion [1], Aggregated Claim [4]

Synonyme: Attribute Assertion (engl.), confirmation de valeur d'attribut

2.8 Attribute Assertion Service

Un Attribute Assertion Service délivre les *confirmations d'attribut* par le biais d'une interface définie.

Synonyme: Confirmation d'attributs Service

2.9 Attribute Provider (AP)

Un Attribute Provider est un registre ou autre répertoire avec un Attribute Service pour la mise à jour des attributs et un Attribute Assertion Service pour la délivrance de confirmations d'attribut.

Synonyme: Attribute Authority (AA), fournisseur de données, fournisseur d'information, OIDC Claims Provider

2.10 Attribute Service

L'Attribute Service tient rapidement à jour un ou plusieurs attributs pour des sujets définis.

2.11 Attribute Based Access Control (ABAC)

Concept d'affectation dynamique des droits d'accès sur la base des attributs du sujet.

2.12 Auditing

a) Vérification de la Policy Compliance

b) Consignation de toutes les actions et décisions visant à garantir la traçabilité

2.13 Valeur d'émission d'un authentificateur

La valeur d'émission est générée comme fonction mathématique (authentificateur ou fonction d'authentification) à partir d'une valeur secrète (clé privée par exemple), d'une ou de plusieurs valeurs d'activation facultatives (PIN ou informations biométriques par exemple), et d'une ou de plusieurs valeurs de saisie facultatives (valeurs aléatoires ou Challenges par exemple).

La qualité de la valeur d'émission est déterminée par le procédé d'authentification sélectionnée ou son implémentation.

Synonyme: valeur d'émission d'un moyen d'authentification

2.14 Authentication Proxy

Un Authentication Proxy associe deux sections de protocole et constitue ainsi un point final de protocole. Il peut transformer et/ou adapter une requête d'authentification et la transmettre à un IdP/AP (voir 2.82). L'utilisateur est authentifié par l'IdP/AP. L'Authentication Proxy peut être une partie d'un Broker (voir **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Exemple dans STIAM: si l'AuthnA(1) n'est pas en mesure d'authentifier un utilisateur, il peut, dans certaines circonstances, agir comme Authentication Proxy, en envoyant lui-même sa propre Authentication Request à un autre AuthnA(2). L'AuthnA(1) peut utiliser la réponse de l'AuthnA(2) pour générer sa propre Response.

2.15 Authentication Service

L'Authentication Service vérifie, à l'aide de moyens d'authentification, si l'accédant (sujet) est bien celui qu'il prétend être.

2.16 Autorité d'authentification (AuthnA)

Une AuthnA met à disposition un Authentication Service auprès duquel peut s'authentifier le sujet. L'Authentication Service effectue les vérifications à l'aide de moyens d'authentification, qui sont délivrés par un Credential Service. Le Credential Service peut être une partie intégrante de l'AuthnA. Les IdP (selon SAML), OpenID Provider et MobileID Provider sont autant d'exemples d'autorités d'authentification.

Synonyme: Authentication Authority (engl.)

2.17 Authentificateur

L'authentificateur est la représentation fonctionnelle des moyens d'authentification du monde

réel. En règle générale, une valeur d'émission est générée avec la fonction d'un authentificateur à partir d'une valeur de saisie (Challenge) et d'une valeur secrète. En fonction de la variante, l'activation de la valeur secrète nécessite un second facteur (PIN).

Synonyme: fonction d'authentification, Authentificator (engl.)

2.18 Authentification

L'authentification est l'opération de vérification d'une prétendue E-Identity d'un sujet selon des règles précises. Le niveau de confiance visé pour l'authentification détermine ces règles.

Cas spécial eIDAS: authentification dynamique (pas de SSO)

Synonyme: authentification[1]

2.19 Demande d'authentification

Une demande d'authentification marque le début d'une authentification du sujet.

Une demande d'authentification est envoyée par le sujet à l'Authentication Service. Celui-ci amorce la vérification de l'E-Identity prétendue.

Synonyme: Authentication Request (engl.)

2.20 Confirmation d'authentification

La confirmation d'authentification est le justificatif délivré par l'Identity Provider (IdP) suite à une authentification positive du sujet. La confirmation d'authentification est valable pour une période donnée et peut contenir un niveau de confiance.

Exemples:

Dans le cas du Security Assertion Markup Language (SAML) [5], la confirmation d'authentification est l'«Authentication Assertion» et est délivrée par le (SAML) Identity Provider.

Dans le cas de l'OIDC [4], la confirmation d'authentification est ce que l'on appelle l'«ID Token» et est délivrée par l'«Authorization Server».

Dans le cas de Kerberos, la confirmation d'authentification est un «Ticket Granting Ticket» (TGT) et est délivrée par le Kerberos Distribution Center (KDC.

2.21 Facteur d'identification

Les facteurs d'identification sont des informations et/ou processus pouvant être utilisés pour authentifier un sujet. Les facteurs d'identification peuvent s'appuyer sur quatre caractères distincts (basé sur la possession, basé sur la connaissance, inhérent ou basé sur le comportement) ou sur des combinaisons de ces caractères:

- facteur d'identification basé sur la possession: repose sur la possession (quelque chose que possède le sujet, Soft-Token/Hardware-Token avec clé privée, passeport ou carte d'identité électronique par exemple),

[1]Un utilisateur s'authentifie auprès d'un système. Un système authentifie un utilisateur.

- facteur d'identification basé sur la connaissance: repose sur les connaissances (quelque chose que le sujet sait/connaît, mot de passe, PIN par exemple),

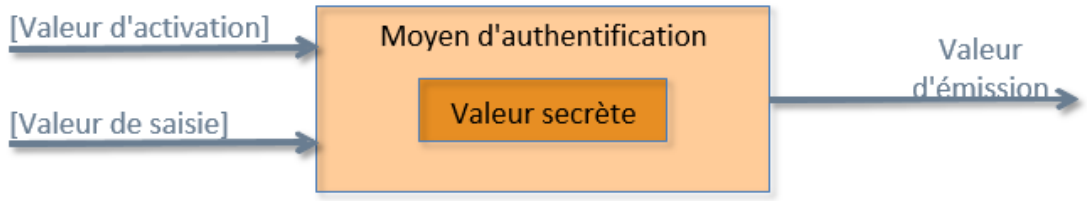
- facteur d'identification inhérent: s'appuie sur une caractéristique biométrique (quelque chose qui est le sujet, comme l'iris, la rétine, empreintes digitales),

- facteur d'identification basé sur le comportement: s'appuie sur le comportement (quelque chose qui singularise le sujet, une façon de signer dynamique par exemple).

Synonyme: caractère d'authentification

2.22 Moyen d'authentification

Un moyen d'authentification est quelque chose que possède un sujet et dont il a le contrôle (habituellement une clé cryptographique, un secret, une caractéristique biométrique ou un comportement spécifique). Un moyen d'authentification ne doit pas forcément exister sous forme matériel, il peut tout aussi bien être un Soft-Token ou une composante de logiciel. Un moyen d'authentification peut utiliser un SFA (*single-factor authenticator*) ou également plusieurs facteurs d'identification MFA (*multi-factor authenticator*) indépendants. La valeur d'émission générée par le moyen d'authentification (Authenticator output ou authenticator response en anglais) est générée par une fonction mathématique (authentificateur ou fonction d'authentification) à partir d'une valeur secrète (clé privée par exemple), d'une ou de plusieurs valeurs d'activation facultatives (PIN ou informations biométriques par exemple), et d'une ou de plusieurs valeurs de saisie facultatives (valeurs aléatoires ou Challenges par exemple). Dans un cas banal, le moyen d'authentification peut être la valeur secrète même (dans le cas d'un mot de passe par exemple). Voir le Tableau 1 pour plus d'exemples.




```
Valeur
d'émission=Fonction d'authentification (valeur secrète,
                                       [valeurs d'activation],
                                       [valeurs de saisie])
```

Figure 1: Fonctionnement schématisé d'un moyen d'authentification

	Mot de passe	Listes de décompte	SMS	OTP	Mobile-ID	SuisseID
Type	SFA	SFA	SFA	(HW-)MFA	HW-MFA	HW-MFA
Valeur de saisie	-	Index	Code envoyé	Seed	Code envoyé	Nonce
Valeur secrète	Mot de passe	Valeur (alpha)numérique	-	Device Key	Private Key	Private Key

	Mot de passe	Listes de décompte	SMS	OTP	Mobile-ID	SuisseID
Valeur d'activation	-	-	-	-	PIN	PIN
Authentificateur	-	Liste des valeurs (alpha) numériques	Téléphone portable	Device	Carte SIM	Crypto-Device
Fonction d'authentification	Aucune ou fct. hash.	Sélection	Lecture et écriture du code envoyé	HMAC	Signature	Signature
Valeur d'émission	Mot de passe, hash du mot de passe	Valeur (alpha)numérique	Code envoyé	Code	Sign (Code envoyé)	Sign (Nonce)
Credential[2]	Mot de passe, hash du mot de passe	Liste des valeurs (alpha)numériques	No. de mobile	No. d'appareil/ Seed	Carte SIM avec no. de mobile/ Public Key	Certificate

Tableau 1: Exemples de moyens d'authentification et Credential correspondant

Synonyme:

- Authenticator (voir NIST 800-63-3 [6]), auparavant désigné comme Token dans NIST 800-63-2 [7].
- Désigné comme identity token ou authentication token par STORK[3]

2.23 Autorisation Service

Le service vérifie, pour la période d'exécution, que les droits relatifs à l'utilisation de l'E-Ressource sont respectés, et permet au sujet d'utiliser la ressource, sous réserve qu'il détienne les droits correspondants.

2.24 Autorisation

L'autorisation est le terme générique couvrant les autorisations grossières et précises (voir 0 et 0).

Synonyme: Authorization (engl.)

[2] Le Credential contient toujours l'identifiant, le nom de l'utilisateur par exemple.

[3] Voir: https://www.eid-stork2.eu

2.25 Backend Attribute Exchange (BAE)

Demande d'attribut en arrière-plan, habituellement par une machine. Un utilisateur n'est pas directement impliqué dans la demande d'attribut, cette dernière se produisant sans son consentement explicite.

2.26 Autorité

Une organisation juridiquement légitime, qui remplit des tâches d'Etat de la Suisse. Les autorités peuvent exister au niveau communal, cantonal ou fédéral et relever du pouvoir législatif, exécutif ou juridique (voir également eCH-0122[4]).

2.27 Utilisateur

Un utilisateur est une représentation technique d'un sujet. D'ordinaire, la notion d'«utilisateur» est utilisée comme représentation d'une personne physique. La représentation technique d'un service est appelée «utilisateur technique».

Synonyme: User (engl.)

2.28 Gestion des identités centrée sur l'utilisateur

Permet à l'utilisateur de choisir des moyens d'authentification et attributs spécifiques pour le traitement dans les demandes d'authentification et d'attribut et lui confie ainsi le contrôle de sa propre identité numérique. Cela ne signifie pas l'utilisateur doit de nouveau approuver explicitement chaque transaction, mais que les données sont toujours intégrées la gestion des identités de l'utilisateur et sont directement liées à son identité numérique.

2.29 Autorisation

L'autorisation correspond à la somme de tous les droits et privilèges d'accès.

2.30 Domaine STIAM (Domain)

Peut être considéré comme domaine un groupe limité de bénéficiaires et de fournisseurs d'informations, qui ont un certain nombre d'attributs et une politique en commun. La sémantique et la syntaxe de ces attributs sont déterminées par les participants du groupe. Il devrait par exemple être possible pour une fédération partielle de se constituer au sein de Suisse-TrustIAM en vue d'échanger uniquement ses identités et attributs connus en interne via la plateforme.

2.31 Moyen de preuve

Un moyen de preuve (dans l'IAM) est un document ou objet provenant d'une source faisant

[4] https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122&documentVersion=1.0

autorité, qui contient des renseignements concernant le requérant. On peut l'utiliser pour vérifier une identité.

Un moyen de preuve doit contenir le nom du requérant. Il peut en outre contenir un identificateur sans ambigüité, une caractéristique physique et biométrique mais aussi n'importe quel autre renseignement sur le requérant. Il devrait contenir des caractères de sécurité rendant toute reproduction difficile.

Exemples:

- acte certifié
- cartes de crédit
- permis de conduite
- pièces d'identité

2.32 Caractéristique biométrique

Une caractéristique biométrique correspond à une caractéristique physique d'une personne qui permet de la distinguer d'autrui de manière suffisante et qui peut donc être utilisée pour identifier cette personne. Une caractéristique biométrique devrait peu changer au fil du temps. Des combinaisons de plusieurs caractéristiques sont tout à fait possibles, par exemple l'enregistrement du visage combiné à la reconnaissance de la voix. L'utilisation des caractéristiques biométriques pour l'authentification présente cependant un inconvénient majeur, à savoir qu'en cas de compromission, elles ne peuvent être déclarées invalides ou de nouveau générées.

Parmi les caractéristiques biométriques les plus importantes, on trouve:

- les empreintes digitales
- la signature (dynamique)
- la géométrie du visage
- la photo du visage
- les motifs de l'iris
- la rétine
- la géométrie de la main
- la géométrie des doigts
- la forme de l'oreille
- la voix (timbre)
- l'ADN
- la frappe au clavier
- la cartographie veineuse

Les personnes physiques sont actuellement identifiées principalement par seulement

- leurs empreintes digitales

- leur iris
- leur rétine
- la géométrie de leur visage
- la photo de leur visage.

Les caractéristiques biométriques peuvent également être classées par fonction, sécurité, possibilité de falsification et convivialité d'application. Le NIST propose une première contribution sur la question sous la forme d'une documentation en ligne «Strength of Function for Authenticators – Biometrics» [8] – SOFA-B en abrégé.

2.33 Broker Service

Ce service fait l'intermédiaire entre le sujet, les ressources et les services de la période d'exécution et fédère les confirmations d'authentification et d'attribut.

2.34 Certificate Policy (CP)

Une Certificate Policy contient les règles d'application d'un type de certificat particulier. Voir également 2.111 Policy et 0 Synonyme: Certificate Authority, Certification Service Provider, Trust Service Provider (TSP)

Synonyme français: service de certification pour les certificats numériques, fournisseur de services de confiance

Certification Practice Statement (CPS).

2.35 Certificate Revocation List (CRL)

Liste des *certificats numériques* délivrés par une (ou plusieurs) CA et qui ont été révoqués. Chaque item de la liste comprend au moins le numéro de série du certificat révoqué ainsi que la date de révocation.

2.36 Certification Authority (CA)

Un Certification Authority est un Credential Service Provider (CSP) spécial comme instance technique, qui émet, renouvelle et révoque des certificats numériques (certificats Public Key, par exemple X.509) comme moyen d'authentification. Voir également 2.1 Fournisseur de Services de certification et 2.42 Credential Service Provider (CSP).

Synonyme: Certificate Authority, Certification Service Provider, Trust Service Provider (TSP)

Synonyme français: service de certification pour les certificats numériques, fournisseur de services de confiance

2.37 Certification Practice Statement (CPS)

Policy utilisée par un fournisseur de services de certification afin de délivrer des certificats. Voir également 2.111 Policy et 2.34 Certificate Policy (CP).

2.38 Client Platform

La Client Platform ou plateforme client est le système ou appareil depuis lequel le sujet initie un processus d'authentification. Il peut s'agir par exemple d'un navigateur sur un PC ou d'une application sur un terminal mobile.

Synonyme: Client, user agent (engl.)

2.39 Community Metadata

Compilation signée de métadonnées d'entité des membres d'une STIAM Community.

2.40 Credential

Un Credential représente une quantité de données (ni matériel, ni autre conteneur physique) servant à associé une identité électronique (E-Identity) à un moyen d'authentification, que le sujet a en sa possession et sous contrôle.

Le Credential est utilisé avec la valeur d'émission du moyen d'authentification comme justificatif de l'E-Identity supposée. En fonction des facteurs d'identification utilisés, le Credential est par exemple le dièse d'un mot de passe, une image d'une caractéristique biométrique ou un certificat (voir également le Tableau 1) qui, au moment de la période de définition, a été associé par un CSP à une E-Identity.

Avant d'utiliser un Credential, il faut contrôler qu'il est bien authentique et digne de confiance.

(voir également ISO 29115 [9], Annexe B et NIST SP 800-63B [10], chap 3).

Synonyme: preuve d'identité

2.41 Credential Service

Le Credential Service délivre et gère les moyens d'authentification. Il permet de renouveler ou de remplacer les moyens d'authentification de manière conviviale. Un moyen d'authentification se rapporte à une E-Identity et est délivré pour un sujet précis.

2.42 Credential Service Provider (CSP)

Un Credential Service Provider est une entité, qui agit comme un émetteur digne de confiance de certificats numériques et autres tokens de sécurité (moyens d'authentification).

Le CSP contient un service d'enregistrement et des services de vérification des Credentials (IdP). Un CSP peut prendre la forme d'une instance publique ou être intégré comme service dans un domaine fermé.

2.43 Période de définition

Le système IAM est mis en place et configuré au cours de la période de définition. Les identités électroniques sont en outre établies. La période de définition englobe ainsi les processus servant à mettre à disposition toutes les informations nécessaires pour tous les composants impliqués ainsi que les composants eux-mêmes.

2.44 Prestataire de services

Le prestataire de service est un Stakeholder dans un système IAM et souhaite que les prestations IAM qu'il propose soient utilisées par autant d'utilisateurs que possible. En outre, il s'efforce de regrouper des services aussi complémentaires que possible afin de préserver toute l'efficacité et le caractère économique du système IAM.

Figure 2: Prestataire de services

La Figure 2 présente le point de vue du prestataire de services sur le système global. Le prestataire de service met sa prestation IAM à disposition du Relying Party. Le sujet peut utiliser la prestation technique du Relying Party à l'aide de cette prestation IAM.

2.45 Certificat numérique

Données structurées, qui confirment le propriétaire ainsi que d'autres propriétés d'une clé publique.

Synonyme: Digital Certificate (engl.), certificat, Public-Key-Certificate

2.46 Chose

Une chose est un objet physique accessible via un réseau (voir 2.104). A l'intérieur du réseau, la chose peut être identifiée sans ambigüité au moyen d'un identificateur. Plusieurs choses, qui sont connectées sur le même réseau, constituent un Internet of Things (IoT ou Internet des objets en français). Les choses peuvent contenir d'autres choses. Une chose peut appartenir à une organisation (voir 2.108) ou une personne physique (voir 2.103).

Synonymes: objet, Thing (IoT)

2.47 Discovery Service (WAYF - Where Are You From)

Le Discovery Service est compétent pour guider l'utilisateur vers un IdP de son choix – à des fins d'authentification.

2.48 Domaine

Communauté ou organisation administrative / technique avec une policy commune (dont l'espace de noms).

2.49 E-Identity

Une E-Identity est la représentation d'un sujet. Une E-Identity (identité numérique) a un identificateur (nom unique), le plus souvent accompagnée d'un certain nombre d'attributs complémentaires, qui peuvent être affectés sans ambigüité à un sujet à l'intérieur d'un espace de

nom (et donc d'un domaine). Un sujet peut avoir plusieurs E-Identities.

Une E-Identity notifiée est une E-Identity, qui doit satisfaire à toutes les exigences préalables stipulées dans eIDAS 910/2014 [11] article 7, comme l'E-ID (voir 2.136) prévue en Suisse par exemple.

Synonymes: identité numérique, Digital Identity, identité électronique, Electronic Identity

2.50 E-Identity Service

L'E-Identity Service délivre et gère des E-Identities concernant les sujets (voir 2.149.

2.51 Propriétés

Les propriétés sont des caractères typiques ou des comportements caractéristiques d'un sujet qui, dans leur globalité, sont spécifiques au sujet.

2.52 Signature électronique

Selon SCSE [2]: «*Données électroniques jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité.*»

2.53 Moyen d'identification électronique

Terminologie d'eIDAS 910/2014 [11]: un «moyen d'identification électronique» est une unité matérielle et/ou immatérielle, qui contient les données d'identification des personnes et sert à l'authentification auprès des services en ligne.

Un moyen d'identification électronique contient des facteurs d'identification, des attributs pour les personnes et a une validité. Dans le cas d'une authentification (dynamique), tout le processus d'authentification du sujet se déroule à l'aide de moyens d'identification. C'est la raison pour laquelle il englobe aussi bien des moyens d'authentification et le Credential que l'IdP. L'authentification avec un moyen d'identification électronique a pour résultat une confirmation d'authentification qui sert à confirmer l'identité du sujet et le succès de l'authentification.

La nouvelle carte d'identité allemande (nCI), y compris Middleware (Appli ID) ou l'infrastructure globale SuisseID composée d'un SuisseID Token, Middleware (pilote de périphérique) et SuisseID IdP, sont autant d'exemples de moyens d'identification électroniques.

2.54 Système d'identification électronique

Terme tiré d'eIDAS 910/2014 [11]: un «système d'identification électronique» est un système servant à l'identification électronique dans le cadre duquel personnes physiques ou morales ou des personnes physiques représentant des personnes morales se voient délivrer des moyens d'identification électroniques.

Un système d'identification électronique notifié doit remplir toutes les conditions répertoriées dans eIDAS 910/2014 [11] article 7.

2.55 Cachet électronique

Une *signature électronique* apposée au nom d'une *entité IDE*. Les cachets électroniques peuvent être créés dans le cadre de processus automatisés.

2.56 Composant destinataire

Le composant destinataire réalise une interface STIAM standardisée pour un RP, qui ne prend pas directement en charge les protocoles STIAM (voir 2.144 **Fehler! Verweisquelle konnte nicht gefunden werden.** Figure 9).

2.57 Entité

Un élément actif d'un système IT, par exemple un processus automatisé ou un certain nombre de processus, un sous-système, une personne ou un groupe de personnes avec des fonctionnalités définies [1].

Organisation avec un rôle défini au sein d'une STIAM Community.

Synonyme: Entity

2.58 Métadonnées d'entité

Les métadonnées d'une Attribute Authority, IdP ou RP pour la définition du rôle d'une entité au sein de la STIAM Community.

2.59 E-Ressource

Représentation numérique d'une ressource (voir 2.122). Une E-Ressource a un identificateur (nom sans ambigüité, souvent URL/URI), qui peut être affecté sans ambigüité à une ressource au sein d'un espace de noms. Une ressource peut avoir plusieurs E-Ressources.

2.60 Service E-Ressource

Le service E-Ressource délivre et gère des E-Ressources pour les ressources.

2.61 Autorisation précise

Octroi ou refus de l'accès à des fonctions ou données individuelles mises à disposition par une ressource.

2.62 Système IAM fédéré

Un système IAM fédéré est une implémentation d'une fédération d'identité (voir Chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**). Pour qu'un système IAM fédéré puisse être établi, les différents domaines doivent se faire mutuellement confiance concernant certains aspects. Cette confiance repose sur des accords explicites et implicites.

Comme l'illustre la Figure 3, un système d'identité fédéré se compose des trois entités Sujet, Relying Party (RP) et d'un Identity Provider (IdP). L'ordre des informations varie en fonction de la variante de protocole utilisée. Toutefois, le sujet communique toujours avec l'IdP comme avec le RP. Le sujet s'authentifie auprès de l'IdP selon un procédé d'authentification primaire à l'aide d'un moyen d'authentification précis (Authenticator). Cet événement est ensuite transmis à la partie ayant confiance via le réseau sous la forme d'une confirmation d'authentification. L'IdP peut joindre à cette confirmation d'authentification des attributs (de personne) supplémentaires concernant le sujet authentifié.

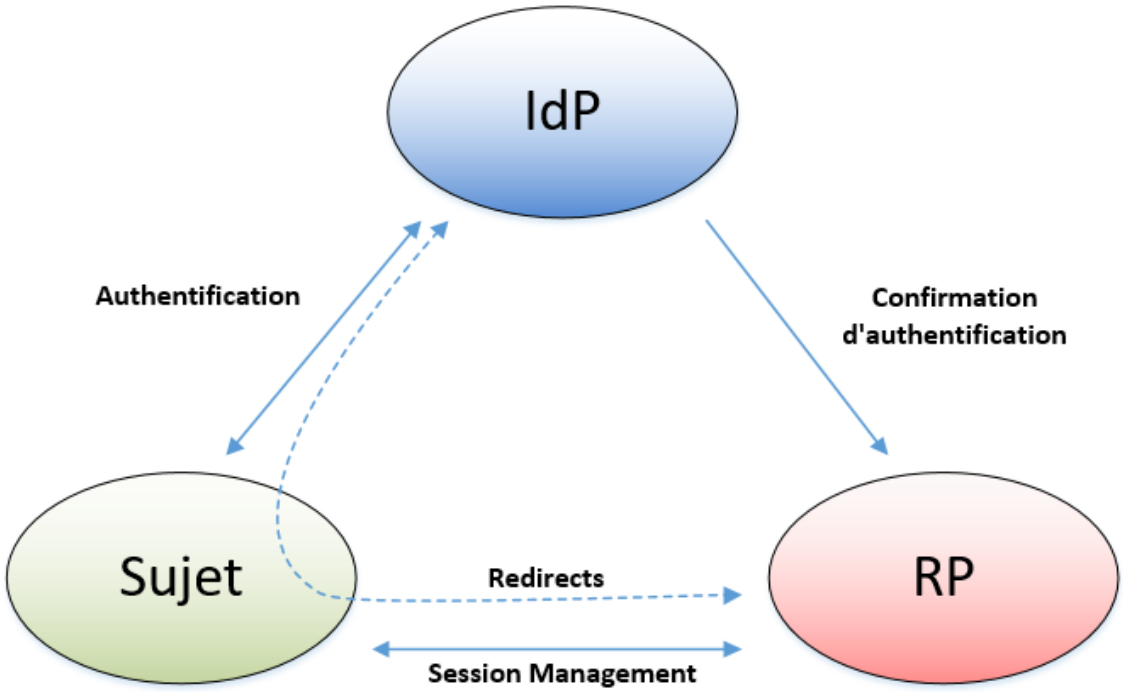


Figure 3: Modèle de fédération d'identité

Système IAM fédéré dans la cyberadministration: dans le cas du système IAM fédéré en cyberadministration, les autorités (voir 0) mettent des ressources à la disposition des sujets de leurs partenaires internes (autres autorités suisses) ou externes (personnes, entreprises, organisations ou autorités d'autres Etats), servant à mettre à disposition en ligne des prestations définies de leur domaine de compétence. Ces ressources doivent être accessibles pour les sujets de leur(s) propre(s) domaine(s) et pour les sujets avec des E-Identities d'autres domaines. Une autorité peut ainsi être un Relying Party (voir 2.120) mais aussi, dans certaines circonstances, un prestataire de services IAM (voir 2.69).

Synonyme: système d'identité fédéré, Identity Federation System (engl.)

2.63 Direction

La direction est un Stakeholder dans un système IAM et souhaite un système IAM stable et performant, qui conviennent à tous les Stakeholders. Elle dirige les prestataires de services IAM et les Relying Parties impliqués et garantit le fonctionnement fiable du système IAM.

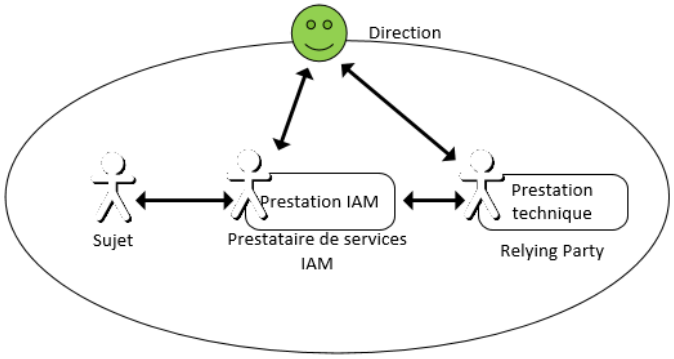


Figure 4: Direction

La Figure 4 présente le point de vue de la direction du système IAM global. La direction souhaite diriger efficacement le système IAM et les Relying Parties et prestataires de services IAM impliqués afin de faciliter l'implémentation et de garantir le fonctionnement fiable. La direction coordonne à cet égard les exigences de tous les Stakeholders dans le système IAM, celles du régulateur et du bénéficiaire de prestation.

2.64 Fonction

Propriété qui assigne à un sujet des tâches, compétences et responsabilités particulières au sein d'une organisation. Un sujet peut avoir plusieurs fonctions (voir rôle).

2.65 Certificat règlementé

Un *certificat numérique* délivré pour une *personne physique* ou une *entité IDE*, qui remplit les exigences de forme correspondantes du SCSE [2]. Les certificats règlementés peuvent par exemple être utilisés pour les cachets électroniques ou pour l'authentification sur un site Web.

2.66 Globally Unique Identifier (GUID)

Un Globally Unique Identifier est une numérotation sans ambigüité et peut être attribué à un sujet.

2.67 Autorisation grossière

Octroi ou refus de l'accès à une ressource au moyen des règles d'accès (voir 2.165).

2.68 Architecture IAM

L'architecture IAM se compose de concepts, de processus, de topologies ainsi que leurs relations au sein du système IAM.

2.69 Prestataire de services IAM

Le prestataire de services IAM est responsable de l'exploitation d'un ou de plusieurs services administratifs IAM selon l'IAM Policy (voir 2.71). On peut établir une distinction entre les spécialisations suivantes qui, toutefois, sont souvent implémentées ensemble. L'exploitation peut être assurée par le prestataire de services IAM même ou bien être confiée à un exploitant externe (outsourcing ou délocalisation). Dans le cas de l'outsourcing, le prestataire de services IAM transmet à l'exploitant les exigences qui lui ont été imposées.

- **Fehler! Verweisquelle konnte nicht gefunden werden.** Service d'enregistrement / Registration Authority (RA)
- 2.42 Credential Service Provider (CSP)

0 L'Identity Mapping est l'opération, pour la période d'exécution, par laquelle des liens LinkedID sont résolus à l'aide du Link Table. Une E-Identity locale peut ainsi être associée à l'E-Identity fédérée.

- Identity Provider (IdP)
- 2.9 Attribute Provider (AP)
- **Fehler! Verweisquelle konnte nicht gefunden werden.** Broker

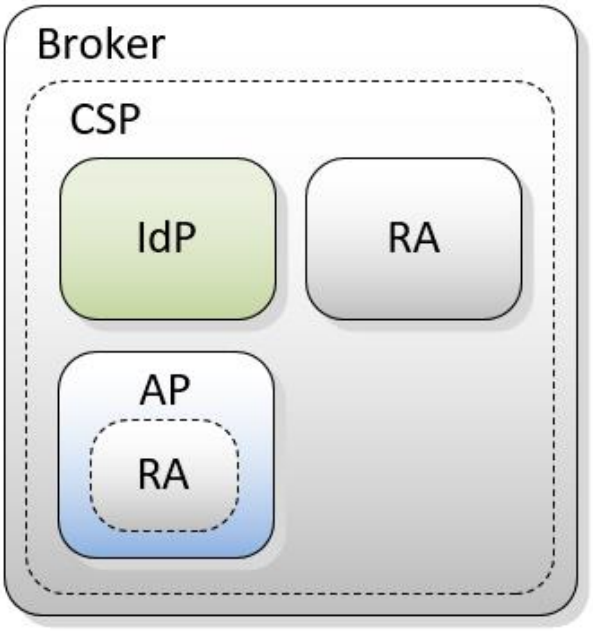


Figure 5: Prestataire de services IAM

La Figure 5 représente tous les prestataires de services IAM dans le cas où ces derniers sont implémentés conjointement.

2.70 Direction IAM

La direction IAM est responsable de la gestion d'un système IAM ou de parties de ce dernier (prestataire de services IAM (voir 2.69) et Relying Party (voir 2.120)).

La **direction IAM** du **système global** gère les prestataires de services IAM et les Relying Parties impliqués (comme pour ITIL [12] par exemple) dans tous les domaines spécialisés tels que Release-Management, gestion de la qualité, gestion des fournisseurs et des consommateurs IAM, Service-Request-Management. Cela peut se produire dans un contexte

aussi bien interne qu'externe par des contrats/SLA des prestataires de services IAM et des Relying Parties externes.

2.71 IAM-Policy

L'IAM-Policy définit les objectifs, principes et limites du système IAM visé.

2.72 IAM Regulator

L'IAM Regulator (ou pilotage IAM) définit les conditions générales juridiques, procédurales, organisationnelles/architecturales et techniques requises dans lesquelles doit être mis en œuvre l'*IAM*. Il tient compte à cet égard des intérêts de tous les Stakeholders et implique tous les autres acteurs dans la définition de manière appropriée.

Les *IAM Regulators* peuvent prendre plusieurs formes et agir aussi bien au sein d'une seule organisation qu'entre plusieurs.

Le **pilotage IAM** définit l'IAM Policy pour un système IAM externe ou interne à l'organisation ou pour des services administratifs IAM.

Le **législateur** définit les conditions générales juridiques dans lesquelles le système IAM global doit opérer et se développer.

L'**organe de normalisation** élabore les normes et directives pour les conditions générales procédurales, organisationnelles/architecturales et techniques.

2.73 Service IAM

Les services IAM remplissent leurs tâches en employant des moyens informatiques. Pour ce faire, ils coopèrent entre eux via des interfaces standardisées, qui utilisent des normes ouvertes (SAML, OIDC, …). Chaque service IAM est fourni par un prestataire de services IAM. L'utilisation est réglée par contrat. Les services IAM ne sont pas des composants de services techniques, cela signifie que lors de la mise en œuvre, un ou plusieurs services IAM peuvent être implémentés par un composant de service technique, ou qu'un service IAM peut être distribué par plusieurs composants de service technique.

Synonyme: IAM Service

2.74 IAM Support

L'IAM Support est responsable de l'ensemble des activités visant à repérer et résoudre les problèmes.

2.75 Système IAM

Un système IAM est une implémentation d'un IAM (voir 2.79), qui est utilisée dans une organisation. Un système IAM peut par principe être indépendant. Les processus d'enregistrement et la gestion des utilisateurs sont des parties intégrantes d'un système IAM.

2.76 Identificateur

Une chaîne de caractères qui définit explicitement une E-Identity ou une E-Ressource, dans le cadre d'un espace de noms (domaine). L'identificateur d'une ressource est souvent une URL/URI.

2.77 Identification

L'identification est une opération pour la période de définition consistant à vérifier l'identité du sujet à l'aide de moyens de preuve dans la plupart des cas. La plupart du temps, l'identification est réalisée par un service d'enregistrement dans le cadre de l'enregistrement.

Synonyme: vérification de l'identité

2.78 Identité

L'identité correspond à l'ensemble des particularités qui caractérisent un sujet et le distinguent de tous les autres en tant qu'individu. Dans le contexte de l'IAM, on utilise principalement l'E-Identity d'un sujet (voir 2.49).

Synonyme: Identity (engl.)

2.79 Gestion de l'identité et de l'accès / Identity and Access Management (IAM)

Tous les processus et systèmes permettant aux sujets, qui en ont besoin aux fins de fonctionnement de leur organisation, d'accéder aux ressources.

Synonyme: gestion de l'identité

2.80 Document d'identité

En Suisse, les documents considérés comme documents ou pièces d'identité sont les suivants:

- passeport,
- carte d'identité suisse,
- carte d'identité reconnue pour l'entrée sur le territoire de la Suisse.

2.81 Fédération d'identités

Une fédération d'identités est une coopération entre différentes entités d'un système IAM par-delà les limites des organisations et des systèmes, sans duplication ni réplication des données d'utilisateurs nécessaires (E-Identities et attributs) contrairement au système IAM répliquant (voir 2.121).

Une fédération d'identités permet de transmettre des informations sur l'authentification d'un sujet et, à titre facultatif, de transmettre des informations d'identité concernant ce sujet via un

réseau.

Synonyme: Identity Federation, IAM fédéré

2.82 Identity and Attribute Provider (IdP/AP)

Un Identity and Attribute Provider (IdP/AP) est un composant, qui combine un IdP (voir 0) et un AP (voir 2.9). Il délivre des confirmations des confirmations d'authentification et d'attributs (voir également 2.144 **Fehler! Verweisquelle konnte nicht gefunden werden.** Figure 9).

Synonyme: Identity Provider/Attribute Authority (IdP/AA), fournisseur d'identité

2.83 Identity Linking

L'Identity Linking est l'opération pour la période de définition par laquelle une LinkedID est associée à une identité numérique sans ambigüité d'un sujet. Les informations nécessaires à cela sont répertoriées dans un Link Table.

2.84 Identity Mapping

L'Identity Mapping est l'opération, pour la période d'exécution, par laquelle des liens LinkedID sont résolus à l'aide du Link Table. Une E-Identity locale peut ainsi être associée à l'E-Identity fédérée.

2.85 Identity Provider (IdP)

Entité qui gère et publie les E-Identities. Un IdP met un Authentication Service (voir 2.15) à disposition.

Synonyme: Authorization Provider, Issuer (U-Prove)

2.86 Personne morale

Les personnes morales sont des organisations définies par l'art. 52 et suivants du CC et par les dispositions applicables du droit des sociétés du CO.

Les personnes morales ne peuvent agir que par le biais de personnes physiques et sont donc toujours associées au minimum à une personne physique (voir 2.149).

2.87 Caractéristique physique

Une caractéristique physique est une caractéristique d'une personne, comme la taille et la couleur des yeux. Les caractéristiques biométriques sont des caractéristiques physiques spéciales (voir 2.32).

2.88 Token cryptographique

Support logiciel ou matériel servant à enregistrer la/les clé(s) privée(s) d'un certificat (exemple de logiciel: Microsoft Certificate Manager sous Windows OS; exemple de matériel: SmartCard, token USB, Hardware Security Module)

Synonyme: certificate token, Cryptographic Token,

2.89 Période d'exécution

Les processus électroniques avec lesquels un sujet – en cas de succès – obtient l'accès aux ressources d'un RP ont lieu pour la période d'exécution.

Synonyme: période d'exécution

2.90 Bénéficiaire de prestations (BP)

Le bénéficiaire de prestations est un Stakeholder dans un système IAM et souhaite à tout moment obtenir, de manière simple et économique, une prestation technique en ligne (commande d'une licence radio ou d'une carte de stationnement par exemple). Il demande à être soutenu en cas de problèmes (usurpation d'identité par exemple) et attend que l'on se conforme aux règles légales.

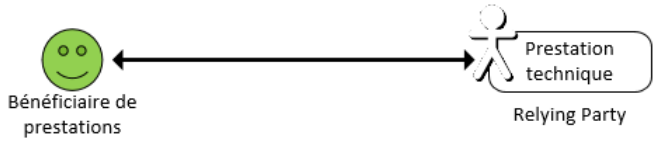


Figure 6: Bénéficiaire de prestations (BP)

La Figure 6 présente le point de vue du bénéficiaire de prestations sur le système global. Le bénéficiaire de prestations souhaite en premier lieu obtenir une prestation technique d'une Relying Party. Pour lui, le système IAM utilisé est secondaire, car seulement un moyen de parvenir à ses fins.

2.91 Fournisseur de prestations (FP)

Le fournisseur de prestations est un Stakeholder dans un système IAM et souhaite proposer des prestations techniques en ligne. Ceci devrait se faire de façon économique, stable, simple et conforme aux règles légales et être utilisés par autant d'utilisateurs que possible. Il souhaite transmettre l'accès et la protection des ressources au prestataire de services IAM en fonction de ses besoins (propension au risque, rentabilité par exemple).

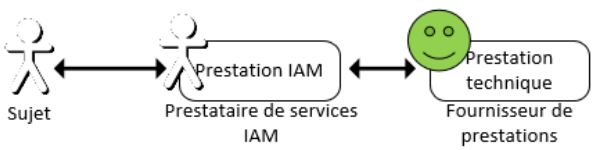


Figure 7: Fournisseur de prestations (FP)

La Figure 7 présente le point de vue du fournisseur de prestations sur le système global. Le fournisseur de prestations souhaite mettre sa prestation technique à la disposition du sujet. La plupart du temps, il ne souhaite pas fournir lui-même les prestations IAM nécessaires à cela (plusieurs services IAM), mais les confie à un prestataire de services IAM (outsourcing).

2.92 LinkedID

Dans le contexte inter-organisations, linkedID permet de mettre en relation les E-Identities de différents domaines. Les E-Identities peuvent être concaténé à n'importe quel graphique dirigé avec des linkedIDs.

2.93 Linking Protocole

L'utilisateur peut associer des IdP ou des AP dans le Link Table de son compte. Pour obtenir le bon identificateur en tant qu'item du Link Table, l'utilisateur doit s'authentifier auprès de l'Authentication Service concerné. Il est ainsi possible pour le Broker et l'IdP ou l'AP de s'échanger un identificateur sans ambigüité.

2.94 Logging Service

Le service documente, pour la période d'exécution, l'utilisation d'un service et met à la disposition de la Support Organisation les informations nécessaires afin de clarifier les problèmes d'utilisation ou les erreurs.

2.95 Look-Up Secrets

Les Look-Up Secrets contiennent une liste de valeurs (alpha)numériques, qui ont été préalablement échangées entre le sujet et le CSP. Une certaine valeur tirée de cette liste doit être indiquée à l'utilisateur à des fins d'authentification.

Les valeurs échangées doivent être générées de façon aléatoire. Elles ne doivent être utilisées qu'une seule fois et présenter une entropie suffisamment élevée.

Exemples: listes de décompte (engl. tally sheet) ou blocs TAN

Synonyme: secret consultable

2.96 Memorized Secrets

Les Memorized Secrets, plus connus sous l'appellation mot de passe ou PIN, sont des valeurs tenues secrètes qui, la plupart du temps, sont choisies par l'utilisateur et gardées dans sa mémoire ou en un autre lieu de conservation sûr. Ils doivent être suffisamment complexes et aléatoires pour éviter qu'un assaillant ne puisse le deviner ou le déduire de quelque manière que ce soit. Les politiques en matière de mot de passe stipulent les règles de longueur, de complexité, de mélange de caractères, de durée de validité et de réutilisation et déterminent ainsi la force des Memorized Secrets.

Exemples: mot de passe ou PIN

Synonyme: secret mémorisé

2.97 Méta-attribut

Elément du schéma d'attribut, spécification de l'attribut s.

2.98 Métadonnées

Un moyen de permettre la confiance et l'interopérabilité technique entre les composants SAML (entités). Peuvent également être utilisées afin d'échanger des informations sur les attributs.

Les métadonnées décrivent les composants des organisations et fournisseurs enregistrés avec leurs points finaux de Federation Service, les certificats et les attributs demandés ou mis à disposition.

Synonyme: Metadata

2.99 Méta-domaine

Domaine régissant la coopération entre deux ou plusieurs domaines.

Synonyme: communauté

2.100 Multi-Factor Cryptographic Devices

Un Multi-factor Cryptographic Device est un instrument physique qui contient une clé cryptographique protégée. Il doit être activé avec un deuxième facteur d'identification (connaissance ou propriété). L'authentification est accomplie par le justificatif de possession et le contrôle de la clé cryptographique.

Exemples: SmartCard, SuisseID

Synonyme: appareil de chiffrage multi-facteurs

2.101 Multi-Factor Cryptographic Software

Un Multi-Factor Software Cryptographic Authenticator est une clé cryptographique conservée sur un disque dur ou autre support semblable. Ce type d'Authenticator doit être activé par un deuxième facteur d'identification. L'authentification est accomplie par le justificatif de possession et le contrôle de la clé cryptographique. Cet Authenticator combine deux facteurs d'identification: possession (clé cryptographique) et un autre secret (possession ou propriété) utilisé pour l'activation.

Exemple: Soft-Token (fichier PKCS#12)

Les exigences sont décrites en détail dans les sources suivantes:
Voir également NIST SP 800-63B [10], chapitre 5.1.7.

Synonyme: logiciel de chiffrage multi-facteurs

2.102 Espace de noms

Champ d'application (entreprise, Etat, communauté spécialisée, communauté linguistique par exemple) pour lequel est définie la signification d'une chaîne de caractères (identificateur

par exemple).

Synonyme: Namespace (engl.)

2.103 Personne physique

Une personne physique est un être humain en tant que sujet de droit. Les personnes physiques peuvent appartenir à une organisation (voir 2.108).

2.104 Réseau

Système d'informations qui est en mesure d'échanger des informations avec différents composants associés.

2.105 Non-répudiabilité

La garantie ou la preuve qu'un sujet s'est engagé à ce que les données et le contenu d'un document électronique soient corrects. La non-répudiabilité constitue un élément important des signatures électroniques qualifiées.

Synonyme: Non-Repudiation, Content-Commitment

2.106 Online Certificate Status Protocol (OCSP)

Un OCSP constitue un protocole servant à interroger le statut de validité d'un certificat numérique. Voir également 0 **Fehler! Verweisquelle konnte nicht gefunden werden.** et 2.35 Certificate Revocation List (CRL).

2.107 OpenID Connect

OpenID Connect 1.0 (OIDC) [4] définit une couche d'identité simple sur la base d'OAuth 2.0 (RFC 6749) [13], qui peut être également utilisé par des appareils mobiles. OIDC utilise le protocole de base OAuth aussi bien pour l'authentification que pour le contrôle des accès. Les Security Tokens utilisés sont les JSON Web Tokens [14].

2.108 Organisation

Une organisation (entreprise, association, administration, groupe de sujets) est un groupe de plusieurs personnes physiques ou de choses. Une organisation peut contenir des (sous-)organisations.

Concernant les organisations, on établit une distinction entre organisations agissantes et non agissantes. Les **organisations agissantes** (identités de groupe par exemple) peuvent s'authentifier et se voir accorder l'accès aux ressources. Les **organisations non agissantes** (personnes morales par exemple) ne peuvent s'authentifier par elles-mêmes, mais uniquement par le biais du sujet correspondant (généralement une personne physique) auquel elle délègue ses droits.

2.109 OTP Devices

Un Single-Factor OTP (One-time Password) Device est un logiciel ou un appareil qui génère spontanément un mot de passe unique (par événement, basé sur le temps).

Un secret embarqué (clé), qui est utilisé pour générer le mot de passe à utilisation unique, se trouve sur l'appareil ou dans l'application. La valeur de saisie peut être l'heure actuelle ou un compteur incrémentiel.

Exemples: SecureID-Token, Google Authenticator, SafeNet mobilePass

Un Multi-Factor OTP Device a besoin d'un deuxième facteur (connaissance ou propriété) sur l'appareil pour activer l'algorithme. Ce deuxième facteur d'identification peut être un pavé numérique intégré, un capteur biométrique (empreintes digitales par exemple) ou une interface informatique directe (USB par exemple).

Exemples: SecureID-Token avec pavé numérique, HID ActivID Token

Synonyme: générateur de mot de passe à usage unique

2.110 Out of Band Authenticators

Out of Band est un appareil physique, qui doit être adressable sans ambigüité et qui peut recevoir des secrets choisis par le CSP en vue d'un usage unique.

Le sujet possède l'appareil, auquel on devrait pouvoir s'adresser via un propre canal privé, qui est utilisé indépendamment du canal primaire pour le deuxième facteur d'identification

L'Out of Band Authenticator peut fonctionner selon deux modes distincts:

1. Le sujet présente le secret, qu'il a reçu via le deuxième canal, au service authentifiant via le canal de communication primaire.
2. Le sujet renvoie au service authentifiant une réponse directement via le deuxième canal de communication.

Exemples: téléphone portable/smartphone avec numéro de mobile et procédure SMS TAN

Synonyme: canal externe

2.111 Policy

Règles et prescriptions stipulées par écrit qui doivent être respectées.

Exemple: une Policy pour un IAM est appelée IAM Policy.

2.112 Signature électronique qualifiée

Une signature électronique qui satisfait aux exigences de forme imposées par la SCSE [2]. Une signature électronique qualifiée peut être considérée comme le pendant de la signature manuscrite dans le monde numérique.

2.113 Certificat qualifié

Un *certificat numérique* délivré pour une *personne physique* et qui satisfait aux exigences de forme imposées par la SCSE [2]. Une *signature électronique qualifiée* doit reposer sur un

certificat qualifié.

(remarque: le règlement UE eIDAS 910/2014 [11] poursuit la définition du certificat qualifié. Il y est notamment stipulé qu'outre le certificat pour la signature électronique qualifié, ce terme couvre également les certificats pour les cachets électroniques et pour l'authentification de site Web. Voir également à ce sujet 0 *Certificat règlementé*.)

2.114 Quality Authentication Assurance (QAA)

Qualité de l'authentification d'une identité numérique selon la norme ISO 29115:2013 [9].

2.115 Droits

Les droits sont des propriétés spécifiques abstraites que le sujet doit posséder afin de pouvoir accéder à une ressource. Celles-ci peuvent être stipulées par des lois ou des contrats par exemple.

2.116 Registres

Répertoires dans le langage administratif, comme le registre des habitants, registre des avocats, registre de l'état civil, registre du commerce etc. Ils sont généralement tenus par des services officiels (administrations, autorités).

2.117 Enregistrement

Processus d'un service d'inscription par lequel un sujet obtient une E-Identity avec le moyen d'authentification et le Credential correspondant. L'enregistrement inclut une *Identification* dans la plupart des cas.

Synonyme: Registration (engl.)

2.118 Service d'enregistrement / Registration Authority (RA)

Un service d'enregistrement est une entité, qui saisit et vérifie suffisamment d'informations concernant le sujet pour pouvoir en vérifier l'identité.

La RA peut être une partie intégrante d'un CSP ou agir comme un service séparé pour le compte du CSP.

2.119 Regulator

Le Regulator est un Stakeholder dans un système IAM et garantit l'interopérabilité (dans le cas de sous-systèmes dirigés de manière autonome en particulier), la solidité et la sécurité du système IAM global.

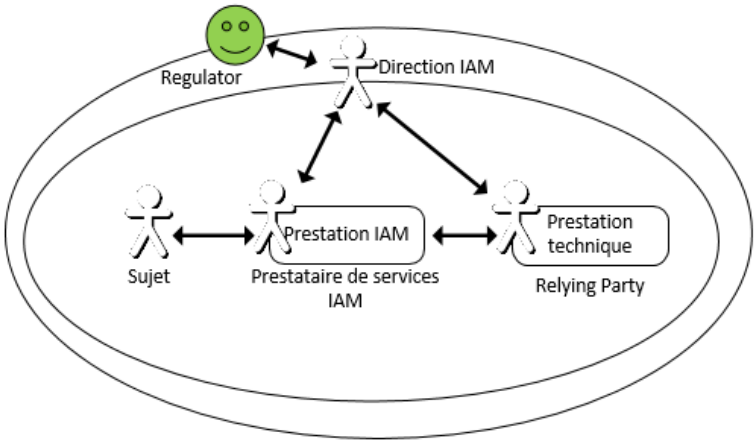


Figure 8: Regulator

La Figure 8 présente le point de vue du Regulator. Le Regulator souhaite, en réunissant les conditions générales correspondantes (lois, normes, stratégies, etc.), promouvoir l'utilisation de systèmes IAM fédérés dans le contexte inter-organisations et, dans le même temps, obtenir une qualité élevée d'aspects non fonctionnels, comme l'interopérabilité, la fiabilité et la sécurité par exemple.

2.120 Relying Party (RP)

Le Relying Party représente les intérêts de la ressource dans le système IAM. Il utilise les services administratifs IAM et traite les informations des prestataires de services IAM (voir 2.69) f pour protéger leurs ressources. Il a besoin, pour vérifier l'autorisation d'un accès aux ressources, d'informations plus détaillées (propriétés pertinentes pour l'autorisation) concernant un sujet, son E-Identity (voir 2.49) et le contexte de l'*accès* (lieu, moment, niveau de sécurité etc.)

Synonyme: bénéficiaires d'informations, consommateur d'informations, consommateur d'identité, fournisseur de solutions, SAML Service Provider

2.121 Système IAM réplicateur

Un système IAM réplicateur gère les données d'utilisateur (E-Identities et attributs) depuis un site central. Lors de l'établissement d'un système IAM réplicateur, les données nécessaires à la création d'une E-Identity sont agrégées (copiées depuis plusieurs sources et persistées) et harmonisées. Au cours de l'exploitation du système IAM réplicateur, les données peuvent être mises à jour périodiquement par les sources.

Contrairement à un système IAM fédéré (voir 0), les sources de données ne sont pas autonomes.

2.122 Ressource

Service ou données auxquels un sujet peut accéder une fois qu'il s'est authentifié et qu'il y a été autorisé sur la base des attributs requis. Cette notion englobe les ressources physiques comme les bâtiments et installations dont l'utilisation est commandée par des systèmes informatiques.

Dans le contexte IAM, on distingue trois types de ressources:

- Ressources **publiques** (non dignes d'être protégées): ces ressources sont en libre accès et aucune authentification n'est nécessaire pour y accéder. Les sites Web d'information (accès en lecture) et les données publiques en sont de bons exemples.
- Ressources **cachées** : ces ressources ne nécessitent pas non plus d'authentification avant l'accès, toutefois la ressource n'est pas disponible de manière générale, mais connue uniquement d'un certain nombre d'utilisateurs. Quiconque connaît l'URL correspondante peut également accéder à la ressource. Les exemples en sont les accès aux Google-Docs ou Doodle-Links.
- Ressources **dignes d'être protégées** (non publiques): ces ressources nécessitent que le sujet accédant se soit préalablement authentifié avec succès.

2.123 Responsable de ressources

Service responsable des ressources gérées par le Relying Party (exemple: responsable d'application, responsable de service, détenteur de données).

2.124 Role based Access Control (RBAC)

Procédé de pilotage et de contrôle d'accès aux données ou services.

Dans le cas de contrôle d'accès basé sur les rôles, un ou plusieurs rôles sont affectés aux utilisateurs ou groupes d'utilisateurs. Un rôle contient un certain nombre d'autorisations (Permissions), qui décrivent les opérations autorisées sur une ressource voir. voir 2.11

Synonyme: contrôle d'accès basé sur les rôles

2.125 Rôle

a) Organisation, sujet: un certain nombre de fonctions qui sont exécutées dans une organisation. Un ou plusieurs rôles peuvent être affectés à un sujet.

b) E-Identity: attributs qui représentent le rôle/les fonctions du sujet

c) Système, entité: tâche et but d'une entité dans une fédération. Un ou plusieurs rôles peuvent être affectés à une entité.

Synonyme: Role (engl.)

2.126 SAML 2.0 Web navigateur SSO Profile

Les profils regroupent les cas d'application spéciaux de SAML. Le profil de navigateur Web SSO (single-sign-on) SAML 2.0 [15] décrit les scenarii d'authentification basés sur le Web, y compris l'Identity Federation, pour le navigateur.

2.127 Protocole SAML

Avec le lancement de SAML, OASIS a défini non seulement le SAML Token, mais égale-

ment un protocole et les Bindings qui spécifient le transfert des Tokens. SAML prend notamment en charge HTTP-POST et HTTP-Redirect comme Request-Response Schema. Outre SAML, on trouve également d'autres protocoles prenant en charge le SAML Token. WS-Federation et WS-Trust en sont deux exemples.

2.128 SAML Token

Un SAML Token contient des informations confirmées concernant l'identité d'un sujet sous une forme standardisée. Le point essentiel d'un SAML Token est l'Assertion. Cette dernière précise le propriétaire du Token, la durée de sa validité, le service qui l'a délivré puis les informations relatives à l'identité du sujet et les éventuels attributs auxquels est relié le Token.

2.129 Security Assertion Markup Language (SAML)

SAML (Security Assertion Markup Language) permet d'échanger de manière standardisée, entre plusieurs participants, des informations concernant l'authentification et des informations sur les attributs à des fins d'autorisation. La norme SAML [14] décrit la syntaxe et les règles concernant la demande, la création et l'échange de SAML-Assertions.

2.130 Security Token

Un paquet de données qui peut être utilisé afin d'autoriser l'accès à une ressource.

Un Security Token contient des informations confirmées concernant l'identité d'un sujet sous forme standardisée (Authentication Statement, Authentication Assertion). Un RP vérifie et valide ces informations afin d'en déduire la décision relative à l'accès.

2.131 Security Token Service (STS)

Security Token Service est un service Web qui délivre des Security Tokens selon la spécification WS-Security [16].

2.132 Elément expéditeur

L'élément expéditeur réalise une interface STIAM standardisée pour relier une Attribut Authority, qui ne prend pas directement en charge les protocoles STIAM, à un STIAM-Hub (voir 2.144 **Fehler! Verweisquelle konnte nicht gefunden werden.** Figure 9).

2.133 Service Level Agreement (SLA)

Désigne un contrat entre donneurs d'ordre et mandataires portant sur des prestations de service récurrentes.

2.134 Service Provider (SP)

Un Service Provider est un prestataire de services IAM (voir 2.69), qui délivre des artefacts pour un sujet authentifié (voir 2.2), – une signature électronique pour un document par

exemple – et les renvoie, sur demande, à un Relying Party (voir 2.120). Le Service Provider est ainsi un terme générique pour un Attribut Provider.

Le Service Provider ne doit pas être confondu avec le SAML Service Provider, qui utilise OASIS dans la spécification SAML et est un synonyme de Relying Party.

2.135 Single Factor Cryptographic Devices

Un Single-Factor Cryptographic Device est un appareil physique qui procède à des calculs cryptographiques au moyen de saisies effectuées sur l'appareil. L'appareil n'a pas besoin, pour ce faire, d'activation par un deuxième facteur d'identification. Pour générer la valeur d'émission, l'appareil se sert de la clé symétrique ou asymétrique enregistré dans sa mémoire. L'authentification est accomplie par le justificatif de possession de l'appareil.

Exemple: YubiKey U2F

Voir également NIST SP 800-63B [10], chapitre 5.1.6.

Synonyme: appareils de cryptage à facteur unique

2.136 Identité électronique reconnue par l'Etat (E-ID)

e-ID désigne l'identité électronique reconnue par l'Etat en Suisse et la législation fédérale relative aux services d'identification électroniques (loi e-ID, voir https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/e-id.html) en définit les conditions générales juridiques et organisationnelles.

2.137 STIAM - SuisseTrust Identity and Access Management

SuisseTrust Identity and Access Management constitue un modèle de système fédéré d'Identity & Access Management et doit être considéré comme une variante possible de solution.

2.138 STIAM Certificate Authority (STIAM-CA)

Une STIAM-CA est une CA acceptée par la STIAM Community.

2.139 STIAM Identity et Attribute Bus

Fait office d'intermédiaire entre le sujet, le RP, l'AuthnA et l'AP concernant les demandes d'authentification et d'attributs.

Reçoit les SAML-Requests du destinataire STIAM et les redirige à l'AuthnA et l'AP compétente. Il reçoit ensuite les Responses de l'expéditeur STIAM et renvoie les informations au bon RP comme SAML-Response agrégée.

2.140 STIAM Community

La STIAM Community est constituée de tous les participants, qui interagissent avec une plateforme STIAM et tiennent compte de la spécification unitaire (voir 2.111).

2.141 Destinataire STIAM

Module de communication en charge de la communication SAML standardisée entre le RP et le STIAM-Hub.

Le destinataire STIAM utilise les services du STIAM-Hub afin de faire authentifier un utilisateur et de se procurer des renseignements supplémentaires concernant celui-ci, qui peuvent ensuite être utilisés afin de piloter l'accès. Le destinataire STIAM définit comment l'utilisateur doit être authentifié et quels attributs sont nécessaires dans quelle qualité afin de permettre l'accès à l'une de ses ressources protégées. Le destinataire STIAM reçoit du STIAM-Hub les informations demandées sous la forme d'une confirmation d'authentification et/ou d'attribut.

2.142 STIAM-Hub

Le STIAM-Hub, en tant que pièce maîtresse de la plateforme SuisseTrustIAM, remplit deux fonctions. En premier lieu, il propose, pour la période de définition, les services administratifs Trust et E-Identity dans lesquels les utilisateurs et les organisations peuvent s'enregistrer sur le STIAM-Hub et, dans un second temps, agit comme Broker (intermédiaire) entre les entités pour la période d'exécution.

2.143 STIAM-IdP

IdP interne d'une plateforme STIAM. Sert à l'enregistrement et à l'initialisation de STIAM Accounts et fournit une authentification des sujets de qualité minimale.

Dans STIAM, un Identity Provider a pour fonction d'authentifier un sujet. Un STIAM-IdP met en œuvre une interface STIAM standardisée avec le STIAM-Hub (voir 2.144 **Fehler! Verweisquelle konnte nicht gefunden werden.** Figure 9).

2.144 Composants STIAM

L'expéditeur STIAM (AP), le destinataire STIAM (RP), les STIAM-IdP, le STIAM-Hub et les STIAM-CSP comptent parmi les composants STIAM. Les composants STIAM sont dotés d'une interface standardisée, qui leur permet de communiquer les uns avec les autres et de se faire mutuellement confiance.

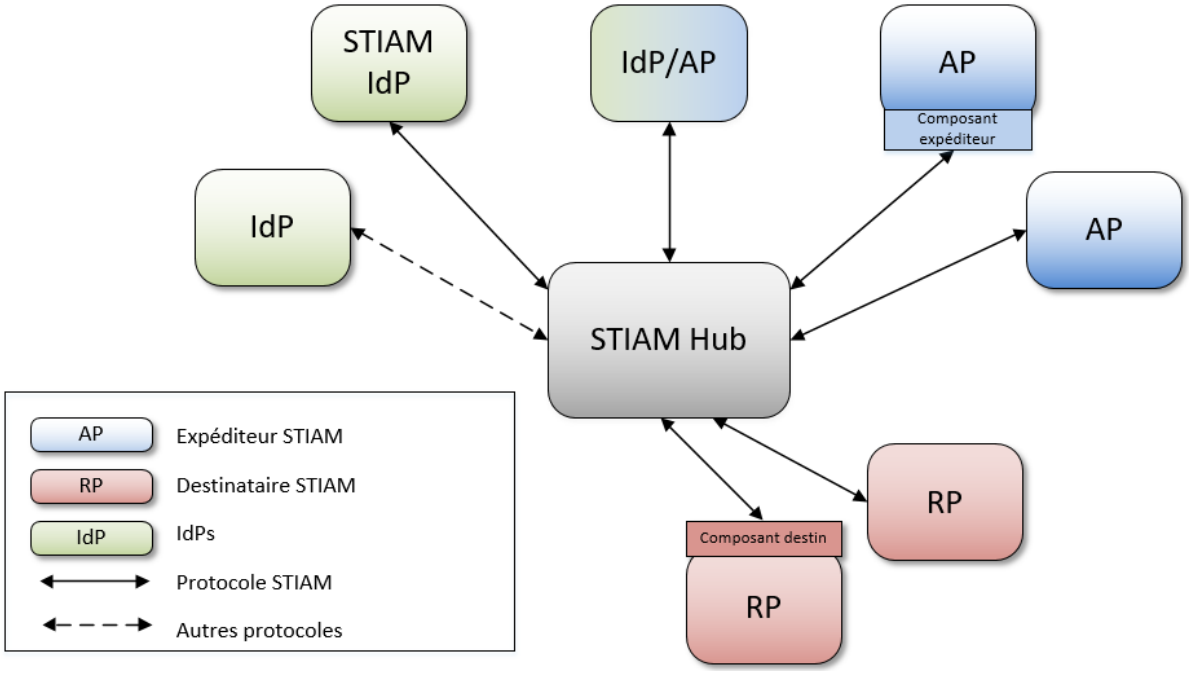


Figure 9: Composants STIAM

2.145 STIAM-Metadata Repository (STIAM-MDR)

Service de renseignement central de la plateforme STIAM qui gère et publie les métadonnées pour la STIAM Community.

2.146 Plateforme STIAM

La plateforme STIAM englobe le STIAM-Hub ainsi que tous les composants supplémentaires propre au STIAM (expéditeur STIAM, destinataire STIAM, STIAM-CSP) qui permettent l'exploitation de la solution fonctionnelle.

2.147 STIAM-RLM (Reporting-Logging-Monitoring)

Les accès aux ressources sont consignés afin de garantir qu'on peut les tracer et les justifier. Le STIAM-RLM doivent permettre, de la même manière, de consigner et de surveiller toutes les opérations dont le STIAM-Hub a assuré la médiation.

2.148 Expéditeur STIAM

Le module de communication qui réalise la communication SAML standardisée entre l'AP et le STIAM-Hub.

L'expéditeur STIAM est une AP (répertoire ou registre en général) qui met à disposition les attributs pour la STIAM Community sous forme standardisée. L'expéditeur STIAM a une interface standardisée avec le STIAM-Hub (voir 2.144 **Fehler! Verweisquelle konnte nicht gefunden werden.** Figure 9).

2.149 Sujet

Un sujet est une personne physique, une organisation agissante (personne morale), une service ou une chose, qui accède ou souhaite accéder à une ressource. Un sujet est représenté par des E-Identities (voir 2.49) dans le monde numérique. Un sujet peut déléguer les droits à un autre sujet.

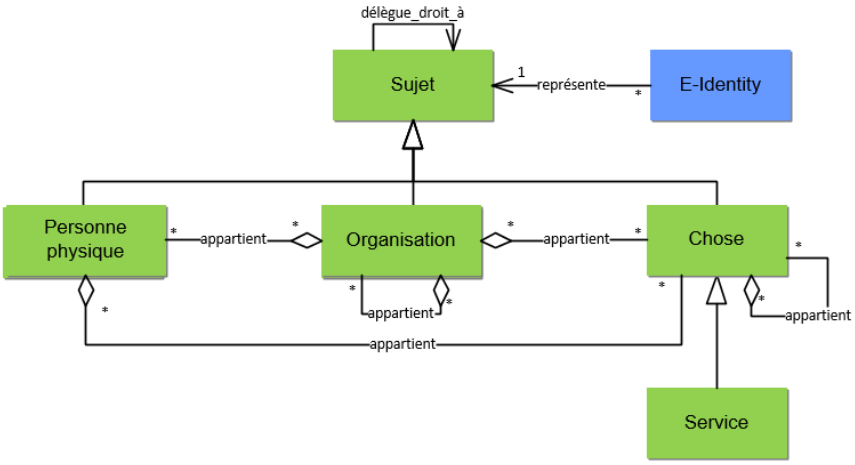


Figure 10: Définition du sujet

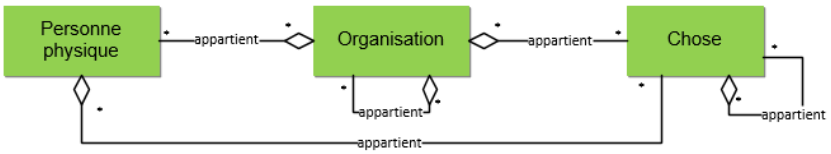


Figure 11: Appartenance des sujets

La Figure 11 montre quels sujets peuvent être contenus dans lesquels (les organisations peuvent contenir plusieurs organisations par exemple).

Un **abonné** (Subscriber en anglais, voir NIST 800-63-3A [17]) est un sujet, qui a reçu un moyen d'authentification par un CSP au terme d'un processus d'enregistrement positif (processus Enregistrer le sujet). Le sujet devient ainsi un participant autorisé à l'Identity Federation Community.

Un **candidat** (Applicant en anglais, voir NIST 800-63-3A [17]), est un sujet, qui souhaite être intégré à l'Identity Federation Community et, à cette fin, passe par le processus Enregistrer le sujet. Si ce processus est concluant, le candidat devient un Abonnent.

Un **porteur** (Bearer en anglais) est un sujet, qui transmet au RP une confirmation d'authentification émise par un IdP.

2.150 Topologie

La topologie d'un système d'Identity Federation décrit l'ordonnancement des différents composants et leurs liaisons logiques.

2.151 Trust Service

Le Trust Service se charge des Relying Parties (voir 2.120) et des prestataires de services IAM (voir 2.69) acceptés et dignes de confiance.

2.152 Trusted Third Party

Instance digne de confiance pour gérer les clés publiques ou certains certificats par exemple.

2.153 Entité IDE

Les entités IDE sont stipulées par l'art. 3.c de la Loi fédérale sur le numéro d'identification des entreprises [18].

Les entités IDE renvoient à toutes les entreprises et institutions qui reçoivent une IDE. Dans le système IDE, le terme d'entreprise s'entend dans une acception large. Par entité IDE, on entend ainsi non seulement les entreprises opérant en Suisse au sens à proprement parler, mais aussi tous les «clientes et clients de l'administration publique» présentant les caractéristiques d'une entreprise ou identifiés à des fins juridiques, administratives ou statistiques.

Pour plus de renseignements concernant le numéro d'identification des entreprises, s'adresser à l'Office fédéral de la statistique[5].

2.154 Verifier

Le Verifier est une partie intégrante de l'IdP. Il compare la valeur d'émission de l'authentificateur avec le Credential et confirme ainsi l'E-Identity supposée du sujet.

2.155 Source faisant autorité

Une source faisant autorité est une source d'information, quelle que soit sa forme, à laquelle on peut se fier dans une situation concrète.

eIDAS 2015/1502: une «source faisant autorité» est une source d'information, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts, pouvant être utilisés pour prouver l'identité.

Les sources fiables peuvent prendre de nombreuses formes différentes, registre, actes, services etc. par exemple.

2.156 Broker

Un Broker propose des services communs, tels qu'administration des métadonnées, IdP-Discovery, Identity Linking ou transformation des confirmations d'authentification et d'attribut (0), pour tous les autres prestataires de services IAM et Relying Parties (2.120) dans une Identity Federation selon le modèle Hub-'n'-Spoke. Une Authentication Proxy est toujours une partie

[5] https://www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises/entites-ide-entreprises.html

intégrante d'un broker (voir 2.14). A titre facultatif, un Broker peut contenir un CSP (2.42). Voir également 2.33 Broker Service et 2.142 STIAM-Hub

Synonyme: Hub, Broker (engl.)

2.157 Confiance

Relation de confiance, définie de façon formelle, la plupart du temps dans le SLA entre les services responsables. La description formelle des critères par exemple, qui doivent être remplis, afin que deux organisations, entités, domaines etc. se fassent mutuellement confiance.

Synonyme: Trust (engl.)

2.158 Niveau de confiance

Le niveau de confiance indique la qualité avec laquelle un sujet a été authentifié. Le niveau de confiance global est déterminé à partir des 4 sous-modèles (niveau de confiance de l'authentification, niveaux de confiance de l'enregistrement, niveaux de confiance du pilotage et niveaux de confiance de la fédération).

Synonyme: niveau de confiance

2.159 Administration

Le terme administration désigne une collectivité publique (offices et autorités, le cas échéant, organismes privés mandatés pour remplir de telles tâches) qui remplit des tâches d'Etat que la loi lui assigne. Le terme administration est un terme d'organisation que ne couvre pas la définition juridique d'une personne physique et morale.

2.160 Répertoire

Collecte systématique d'informations ayant des caractères communs.

2.161 Révocation

Une révocation de certificat est une déclaration d'invalidité d'un certificat numérique. Des moyens d'identification électroniques peuvent également être révoqués de manière analogue.

Synonyme: révocation, Revocation (engl.), blocage

2.162 WS-Federation

WS-Federation dans la version actuelle 1.2 1.2 [16] fait également partie de la spécification WS-* et accroît WS-Trust avec la possibilité d'échanger des Security Tokens également à différents domaines, la norme prenant en charge plusieurs Identity Providers. Concernant WS-Federation, le format SAML-Token peut être utilisé comme Security Token.

2.163 WS-Trust

Le Web Service Trust (WS-Trust) [16] spécifié par OASIS dans la version 1.4 fait partie de la spécification WS*, qui met à disposition un Framework (cadre) pour l'échange, en toute sécurité, de messages Web Service. Dans le cas de WS-Trust, il s'agit d'une norme qui prend en charge l'interopérabilité des Security Token en définissant un protocole pour les exigences et les réponse.

2.164 Service d'entrée

Le service vérifie que les règles d'entrée sont bien respectées et autorise l'entrée au sujet, dès lors que les règles applicables sont respectées.

Synonyme: Access Service (engl.)

2.165 Règles d'entrée

Les responsables des ressources définissent les règles d'entrée pour leurs E-ressources. Les règles d'entrée définissent les conditions dans lesquelles un sujet se voit accorder l'entrée dans une ressource (voir 2.122) ou ses fonctionnalités (autorisation grossière), suite à une authentification positive et à la confirmation de certains attributs par exemple.

2.166 Service de règles d'entrée

Le service de règles d'entrée gère les règles d'accès à une E-ressource (voir 2.52). Les règles sont définies sur la base de l'authentification ou d'attributs.

2.167 Accès

Interaction avec une entité afin de manipuler ou d'utiliser une ou plusieurs ressources [1].

Les accès sont enregistrés afin de garantir la traçabilité et la possibilité d'en justifier.

Synonyme: Access (engl.)

2.168 Contrôle d'accès

Surveillance et pilotage de l'accès aux ressources. Le but est de garantir l'intégrité, la confidentialité et la disponibilité des informations.

Synonyme: Access Control (engl.)

2.169 Droit d'accès

Les responsables des ressources définissent les droits d'accès pour leurs E-Ressources. Les droits d'accès définissent les conditions dans lesquelles un sujet est autorisé à utiliser les différentes fonctionnalité d'une ressource (autorisation précise), par exemple après authentification et confirmation réussies d'attributs particuliers.

2.170 Service de droit d’accès

Le service de droits d’accès gère les droits pour l’utilisation d’une E-Ressource. Les droits sont définis sur la base de l’authentification, des attributs, du contexte d’accès (lieu, moment, niveau de sécurité etc.) ou de modèles propres (groupes, rôles, autorisations individuelles).

3 Exclusion de responsabilité - droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des réglementations applicables.

4 Droits d'auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s’engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu’à l’association **eCH**, pour une utilisation et un développement sans restriction dans le cadre des buts de l’association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s’appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

[1] S. Cantor, J. Hodges, F. Hirsch, R. Philpott, R. S. a Security, J. Hughes, A. Origin, H. Lockhart, B. E. a Systems, M. Beach, R. Metz, B. A. Hamilton, R. Randall, T. Wisniewski, I. Reid, P. Austel, R. L. B. Morgan, P. C. Davis, J. Kemp, P. Madsen, A. Anderson, and S. Microsystems, “Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0,” *Oasis Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

[2] Schweizerische Eidgenossenschaft, “Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES),” 2016 [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20131913/index.html

[3] N. Klingenstein, “Attribute aggregation and federated identity,” *SAINT - 2007 Int. Symp. Appl. Internet - Work. SAINT-W*, 2007.

[4] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, “OpenID Connect Core 1.0 incorporating errata set 1,” 2014 [Online]. Available: http://openid.net/specs/openid-connect-core-1_0.html

[5] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, and T. Scavo, “Security Assertion Markup Language (SAML) V2.0 Technical Overview (OASIS),” 2007 [Online]. Available: https://www.oasis-open.org/committees/security/docs/draft-sstc-baker-saml-arch-00.pdf

[6] J. L. F. Paul A. Grassi, “DRAFT NIST Special Publication 800-63-3,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed: 22-Jun-2017]

[7] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, W. E. Burr, D. F. Dodson, and R. A. Perlner, “NIST Special Publication 800-63-2 Electronic Authentication Guideline,” 2003 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[8] NIST, “DRAFT Strength of Function for Authenticators - Biometrics.” [Online]. Available: https://pages.nist.gov/SOFA/SOFA.html. [Accessed: 03-Nov-2016]

[9] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenberg, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.

[10] J. P. R. Paul A. Grassi, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, James L. Fenton, “DRAFT NIST Special Publication 800-63B,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accessed: 22-Jun-2017]

[11] D. A. S. Europ, I. Parlamentder, R. A. T. D. E. R. Europ, and I. Union, “VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, (eIDAS),” 2015.

[12] Wikipedia, “IT Infrastructure Library.” [Online]. Available: https://de.wikipedia.org/wiki/IT_Infrastructure_Library

[13] E. D. Hardt, “The OAuth 2.0 Authorization Framework [RFC 6749],” 2012 [Online]. Available: https://tools.ietf.org/html/rfc6749

[14] M. Jones, J. Bradley, and N. Sakimuar, “JSON Web Token (JWT),” 2015 [Online]. Available: https://tools.ietf.org/pdf/rfc7519.pdf

[15] S. Cantor, J. Hodges, F. Hirsch, R. Philpott, R. S. a Security, J. Hughes, A. Origin, H. Lockhart, B. E. a Systems, M. Beach, R. Metz, B. A. Hamilton, R. Randall, T. Wisniewski, I. Reid, P. Austel, R. L. B. Morgan, P. C. Davis, J. Kemp, P. Madsen, A. Anderson, and S. Microsystems, “Profiles for the OASIS Security Assertion Markup Language (SAML),” *Oasis Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[16] K. Lawrence, C. Kaler, A. Nadalin, M. Goodner, and M. Gudgin, “WS-Trust 1.4,” *Oasis Stand.*, no. April, 2012 [Online]. Available: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html

[17] J. L. F. Paul A. Grassi, Jamie M. Danker, William E. Burr, “DRAFT NIST Special Publication 800-63A,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63a.html. [Accessed: 22-Jun-2017]

[18] D. Bundesversammlung and D. S. Eidgenossenschaft, *Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG)*. 2011 [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20082601/index.html

Annexe B – Collaboration & vérification

Gruoner Torsten	Administration fédérale – DFF – UPIC
Hassenstein Gerhard	Haute école spécialisée bernoise, TI
Heerkens Marc	Administration fédérale – DFF – UPIC
Kunz Marc	Haute école spécialisée bernoise, TI
Laube-Rosenpflanzer Annett	Haute école spécialisée bernoise, TI
Leimer Bojan	Haute école spécialisée bernoise, TI
Müller Adrian	ID Cyber-Identity Ltd
Selzam Thomas	Haute école spécialisée bernoise, FBW
Spichiger Andreas	Haute école spécialisée bernoise, FBW
	Groupe spécialisé eCH IAM

Annexe C – Abréviations

AA	Attribute Authority
AP	Attribute Provider
CA	Credential Authority
CSP	Credential Service Provider
E-ID	Identité électronique reconnue par l'Etat
eIDAS	Règlement (UE) no. 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
UE	Union européenne
FIDO	Fast IDentity Online
HTTP	Hypertext Transfer Protocol
HW-MFA	Hardware Multifactor Authentication
IAM	Identity and Access Management
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KDC	Kerberos Distribution Center
MFA	Multi Factor Authentication
NIST	National Institute of Standards and Technology
nCI	Nouvelle carte d'identité
OIDC	OpenID Connect
OTP	One-time Password
PIN	Numéro d'identification personnel
RA	Register Authority / service d'enregistrement
RP	Relying Party
SAML	Security Assertion Markup Language
SFA	Single Factor Authentication
SMS	Short Message Service
SSO	Single Sign-on
STORK	Secure idenTity acrOss boRders linKed
TGT	Ticket Granting Ticket
TSP	Trust Service Provider
UID	Unique Identifier
URL	Uniform Resource Locator
CC	Code civil suisse

Annexe D – Liste des illustrations

Annexe E – Liste des tableaux